B.5 INDIRECT HANDLING RATE

Long Distance Travel and ODC costs incurred may be burdened with the contractor's indirect handling rate in accordance with the Contractor's disclosed practices and consistent with FAR 31.2. If no indirect handling rate is allowable in accordance with the Contractor's disclosed practices, no indirect handling rate shall be applied to or reimbursed on such costs.

B.6 CIO-SP3 LABOR CATEGORIES

When responding to a request for proposal under task order solicitations, regardless of contract type, the contractor shall identify both Prime and Subcontractor labor using the CIO-SP3 Labor Categories. Standardized CIO-SP3 labor categories apply to this solicitation. A contractor may propose a new or different skill level category at the task order level by providing a detailed justification for the new/different skill level category. The Contracting Officer will determine whether circumstances warrant the use of unique professional skills.

Section C – Statement of Work

C.1 BACKGROUND

The Government National Mortgage Association (Ginnie Mae) supports affordable housing financing by funding the Government's loan market so that millions of Americans can buy, refinance, and rent homes. Through its Mortgage Backed Securities (MBS) programs, Ginnie Mae guarantees privately issued securities backed by pools of mortgages insured or guaranteed by the Federal Housing Administration (FHA), the Department of Veterans Affairs (VA), the Rural Housing Service of the Department of Agriculture (RHS), or HUD's Native American Program (PIH). Ginnie Mae guarantees the registered holder of the securities the timely

payment of scheduled monthly principal and interest payments, loan prepayments and early recoveries of principal on the underlying mortgages.

In February 2010, the Federal Data Center Consolidation Initiative (FDCCI) was created to reverse the historic growth of Federal data centers. The FDCCI seeks to curb this unsustainable increase by reducing the cost of data center hardware, software, and operations; shifting IT investments to more efficient computing platforms; promoting the use of Green IT by reducing the overall energy and real estate footprint of government data centers; and increasing the IT security posture of the government. In December 2010, The Federal Government's 25 Point Implementation Plan to Reform Federal IT was completed which included a "Cloud First Approach". This required federal agencies to identify and move services to the cloud. Ginnie Mae has been using the Data Center Support services dating back to 2012.

However, as of August 1, 2016, the FDCCI is superseded by the Data Center Optimization Initiative (DCOI) which requires agencies to develop and report on data center strategies to consolidate inefficient infrastructure, optimize existing facilities, improve security posture, achieve cost savings, and transition to more efficient infrastructure, such as cloud services and inter-agency shared services.

Ginnie Mae has begun modernization and virtualization efforts designed to better utilize IT resources. This requirement includes migrating legacy applications and databases residing on dedicated physical servers to virtualized servers where possible, and upgrading end of life systems and software to current application operating systems and versions. Virtualization and modernization efforts are not expected to be completed prior to contract award. The Contractor shall work with current providers to complete virtualization and modernization of servers during the migration. If not possible, physical infrastructure shall be utilized.

The objective of cloud migration is to: 1) reduce overall spending on data center hardware, software, and operations; 2) reduce overall IT operations spending for the government through greater leveraging of shared services; 3) improve IT efficiencies, agility, and innovation; 4) shift Government focus from asset ownership to service management; 5) shift IT investments to a more efficient computing platform, including cloud-based solutions; 6) promote the use of Green IT by reducing the overall energy and real estate footprint of government data centers; 7) decrease the number of physical servers in Ginnie Mae's data centers; 8) consolidate and reduce software licensing costs; 9) decrease total information technology energy use; and 10) Support IPV6 transition and implementation where required.

C.2 PURPOSE

Ginnie Mae is implementing an IT Consolidation Program in support of the DCOI, and has a bona-fide need to procure a contract to host, secure, operate and maintain Ginnie Mae's critical enterprise-wide IT infrastructure. Transitioning to a consolidated infrastructure and cloud hosting will benefit the Government and assist Ginnie Mae with accomplishing its mission more efficiently and effectively by reducing capital expenditures, improving IT agility and scalability, reducing computing needs, and provide new approaches to disaster recovery.

C.3 SCOPE

Ginnie Mae requires information technology services implementation of an IT consolidation program. The following services to be provided by the contractor are as follows: program management, information technology architecture design, systems analysis, telecommunications, cyber security, data center services, hardware/software/maintenance, configuration of systems, software licensing, cloud services, hosting services, and disaster recovery service. The primary place of performance will be at the contractor facility. Travel is anticipated for this acquisition based on the following: 1) During the (2) year base period travel will be required in order to support the (3) existing hosting provider's transition of data (i.e. NaviSite, Deloitte, and Bank of New York and Mellon (BNYM)); the contractor will be traveling frequently to New Jersey, Tennessee, California and Massachusetts where the data centers are located. 2) Re-occurring travel is anticipated during the option periods for periodic meeting and site visits.

The Government highlights three areas of high priority within this scope where a solution that adheres to all Government and Industry Standards are solicited: 1) project planning to effectively transition services from multiple contracts into one task order. The delivery of a detailed strategic transition plan and timetable that maps the course for executing an integrated approach to engineering, securing and operating critical IT service delivery, and the establishment of basic project processes to manage the new task order throughout its lifecycle; 2) the contractor shall provide the consolidation and integration of the engineering, design, security, and Operations and Maintenance (O&M) of the infrastructure and network perimeter (includes but is not limited to multiple sets of firewalls, switches, routers, caching servers, antispyware/antimalware/antivirus, SMTP email antivirus/SPAM filtering, web filtering), Cloud services, and 3) the contractor shall create a seamless and integrated incident management and problem resolution solution to improve the quality of service and decrease the time to resolve for the Enterprise Data and Technology Services (EDTS) consolidated customer base.

C.4 CURRENT INFORMATION TECHNOLOGY (IT) ENVIRONMENT

There are existing conditions within Ginnie Mae's current environment which will have a direct impact on the overall acquisition. While the requirement does not necessitate the need for contractor to have system compatibility with existing systems and environmental infrastructure, all offerors shall have the capability to migrate legacy systems residing on current dedicated physical servers to virtualized servers, and upgrading end of life hardware and software to current application operating systems and versions.

C.4.1 GINNIE MAE MAJOR APPLICATIONS

Ginnie Mae's current infrastructure technology portfolio consists of seven key systems (major

applications), and are as follows:

#	System Acronym	System Name	Description	Hosting Owner	Operating Environments
1	**RFS Apps:** [PA/EF, CRA, CAVS, MAS, WHFIT, Disclosure, GPADS/CWIS, CM, IPA, eNOTE HRA]	Reporting and Feedback System	The RFS implements new reporting and feedback functions delineated in Ginnie Mae's Business Process Integration (BPI) ideal process vision. RFS supports centralized data collection and feedback for all MBS post settlement accounting and reporting. Ginnie Mae issuers will upload reported data using sFTP to RFS for data collection, quality checking, data reconciliation, exception reporting to issuers, and final storage in a central data store.	Managed Data Center – NaviSite ; and Master Business Service Administrative Agent (MBSAA) - BYBM	DEV, DR, PRD, SIT, TRN, TST, UAT (Virtualized and Physical)
2	**GMEP**	Ginnie Mae Enterprise Portal	The GMEP is a General Support System that provides a single access point for Ginnie Mae issuers and other business partners to Ginnie Mae's business applications, data, and documentation via portlets.	Pool Processing Agent (PPA) – Deloitte	DEV, DR, PRD, SIT, TRN, TST, UAT (Virtualized and Physical)
3	**GNMA-WS**	Ginnie Mae Web Services	Ginnie Mae's public facing website that supports eGovernment initiatives.	Managed Data Center – NaviSite	DEV, DR, PRD, TST (Physical)

#	System Acronym	System Name	Description	Hosting Owner	Operating Environments
4	**GFAS**	Ginnie Mae Financial & Accounting System	Ginnie Mae's Financial and Accounting System is a PeopleSoft application that tracks and records all accounting transactions and contains date necessary for its financial statements.	Managed Data Center – NaviSite	DEMO/TST/DEV, DR, PRD (Virtualized and Physical)
5	**GNET**	GinnieNET	GinnieNet enables Ginnie Mae to receive pool information from issuers and document custodians electronically, thus eliminating paper submissions.	PPA - Deloitte	DEV, DEV/TST/TRN, DR, PRD, TST/TRN, UAT (Virtualized and Physical)
6	**IPMS** Pool Processing Agent, Central	Integrated Pool Management System	The Integrated Pool Management System functions as the core processing system for Ginnie Mae pool and MBS certificates/book entry positions. It contains pool,	PPA – Deloitte	DR, PRD, PRD/DEV, UAT/DEV (Virtualized, Physical and Mainframe)

#	System Acronym	System Name	Description	Hosting Owner	Operating Environments
	Processing and Transfer Agent, Pool Reporting System		investor and issuer information.		
7	**Salesforce**	WorkFlow Management Solution with Salesforce.com	Ginnie Mae leverages the Salesforce.com platform to provide an end-to-end relationship management and workflow automation capabilities such as Applicant review, Issuer management; and governance and administration functions. Only Managed Data Center-hosted environments in-scope.	Salesforce Cloud Platform, Managed Data Center – NaviSite	DEV, DR/STG, PRD, SIT, QA/TRN (Virtualized and Physical)

Note: The Reporting and Feedback System (RFS) is a major application that replaces the Mortgaged Backed Securities Information System (MBSIS) and related systems.

C.4.2 GINNIE MAE IT ENVIRONMENT

Ginnie Mae utilizes several environments as part of the overall systems development and integration process. The environments and associated descriptions are listed below:

Demonstration (DEMO): Contains sample configuration and transaction data. The DEMO environment is leveraged to conduct additional testing for new function functionality. It is also used to apply patches released by PeopleSoft for testing prior to migrating to other environments.

Development (DEV): The development (DEV) environment is used by contractors and Ginnie Mae to conduct development and integration testing prior to official system testing in SIT and UAT. Code is promoted here from the developer's local machine and tested to ensure correctness. Once code is successfully integrated and tested here, it is considered ready for system testing.

Disaster Recovery (DR): The disaster recovery environment is configured to support Ginnie Mae applications in case the primary hosting facility is rendered inoperable. The disaster recovery environment will include a dedicated production environment including dedicated servers for each production (PROD) application. Connectivity will be secured through a secure VPN internet connection.

Production (PRD): This is the production environment for Ginnie Mae. Only software that has passed system testing and been fully accepted and base-lined by Ginnie Mae can be promoted to

production. These are considered the critical servers hosting live data and systems for use by the public and require the highest up-time.

Quality Assurance (QA): The QA environment is for testing upgrade procedure against data, hardware, and software that closely simulate the Production environment and where intended users test the resulting application.

Staging (STG): The STG Environment is part of the CipherCloud application and is hosted by Managed Data Center and Salesforce.com. This environment mirrors the production environment and its purpose is to enable Quality Assurance tests after the DEV environment before moving to the PROD environment.

System Integration Testing (SIT): The SIT testing environment is where pieces of Ginnie Mae application code are uploaded and tested for interoperability with other applications. The code is integrated after normal software testing is conducted and approved.

Test (TST): The Test environment is reserved for testing single pieces of Ginnie Mae application code. Prior to moving the code through SIT and UAT testing, the code must be tested and approved in this environment.

Training (TRN): The Training Environment is designated for educating end users on how to operate Ginnie Mae applications. The Training environments are also paired with QA environments in some instances. These environments are typically closed off from PROD environments and enable users to experiment and learn.

User Acceptance Testing (UAT): The UAT Environment is where Ginnie Mae applications are tested to confirm that the functionality is working properly for end users. Code will have already passed through the TST and SIT environments to reach this stage of the Software Development Lifecycle.

C.4.3 GINNIE MAE SYSTEM SERVER AND OPERATING SYSTEMS INVENTORY (OS)

Ginnie Mae's applications and their supporting services are hosted across a pool of physical and virtual servers which are managed by third-party vendors through the current Managed Data Center NaviSite Contract and Pool Processing Agent (PPA) Deloitte contract; at multiple locations in the United States. **(See Attachment A)**

C.5 TASKS

The following tasks are required in support of this TOR and are detailed below:

C.5.1 TASK 1 – PROGRAM MANAGEMENT

The Contractor shall provide program management support under this TOR. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Statement of Work (SOW). The contractor shall identify a Program Manager (PM) by name that shall provide management, direction, administration, quality assurance, and leadership of the execution of this TOR.

The Contractor shall facilitate Government and contractor communications; use industry best standards and proven methodologies to track and document TOR requirements and activities to allow for continuous monitoring and evaluation by the Government; and ensure all support and requirements performed are accomplished in accordance with the TOR. The contractor shall notify the Contracting Officer Representative (COR) and Technical Point of Contract (TPOC) of any technical, financial, personnel, also general managerial problems encountered throughout the TO period of performance (PoP).

The Contractor shall recommend the overall communication management structure to provide collaborative, responsive interfacing with the Government and a mechanism to facilitate rapid problem resolution and approval of contractor recommendations by the required authority. The contractor shall ensure that Information Technology Infrastructure Library (ITIL) methodologies are incorporated into the Program management structure and guide the overall execution of the requirements.

The Contractor shall follow sound program management practices (i.e. Project Management Body of Knowledge (PMBOK ®) or an industry equivalent) and adhere to the program, project, and the applicable CMMI processes and SOPs developed by the operating units.

C.5.1.1 SUBTASK ONE – COORDINATE POST AWARD/KICK-OFF MEETING

The Contractor shall schedule and coordinate a Project Kick-Off Meeting at the location approved by the Government within ten business days after contract award. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved in the TO. This meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the directorates, other relevant Government personnel, and the COR.

The contractor shall provide the following at the Kick-Off Meeting:

a. Draft Transition-In Plan
b. Draft Program Management Plan
c. Quality Control Plan (QCP)

C.5.1.2 SUBTASK TWO – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor PM shall develop and provide an MSR using Microsoft (MS) Office Suite applications, by the first of each month via electronic mail to the Technical Point of Contact (TPOC) and the COR. The MSR shall include the following:

a. Activities during the report period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the tasks.
b. Problems and corrective actions taken to include any technical, financial, personnel, or problems with performance. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearance, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
g. Accumulated invoiced cost for each CLIN up to the previous month.
h. Projected cost of each CLIN for the current month.
i. Contractor risks and issues related to managing the contract.
j. Asset Management reports annotating all assets to include hardware, software, licenses, telecommunications, warranty, support and services.
k. Monthly Infrastructure Operations Report (Virtualization, Utilization, Storage, Uptime/downtime, patching, Infrastructure incidents, service availability, LAN/WAN utilization)

The monthly status report is due on the 1st business day of each month.

Deliverable associated with this task include:

1. Monthly Status Report

C.5.1.3 SUBTASK THREE – CONVENE TECHNICAL STATUS MEETING

The contractor PM shall convene a monthly Technical Status Meeting with the TPOC, COR, and other vital Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting. The contractor shall provide a Weekly Status Report that includes at a minimum the following:

a. Project Status
b. Schedule Changes
c. Key Weekly Activities
d. Issues & risks
e. Other relevant information

C.5.1.4 SUBTASK FOUR – PREPARE A PROGRAM MANAGEMENT PLAN (PMP)

The Contractor shall develop, deliver, update and comply with a PMP that lays out its approach, timeline, and tools to be used in the execution of the contract. The PMP shall provide the foundation for managing the program and shall at a minimum describe the proposed management approach, detailed Standard Operating Procedures (SOPs) for all tasks including milestones, tasks, and subtasks required in this TOR, overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations. The PMP must comply with the HUD PPM process.

Deliverables associated with this task include:

1. **Draft & Final Program Management Plan** - The contractor shall provide the Government with a draft PMP on which the Government will make comments. The contractor shall update the draft PMP submitted and provide a final PMP (10) workdays after receipt of Government comments. The PMP is an evolutionary document that shall be updated annually at a minimum.
2. **Communication Plan** – The contractor shall prepare a Communications Plan that describes in detail the modes, methods, and messages provided to keep entity stakeholders informed of the program's progress. This plan shall identify, at a minimum, individuals or groups, the mode of communication used with each group, the nature of the message (summary and detail), and the frequency and timing of the communication. The contractor shall update the plan upon changes to stakeholder groups or communications needs. The contractor shall prepare communications content and/or materials as defined in the Communications Plan.
3. **Risk Management Plan** - The contractor shall establish and maintain a Risk Management Plan to include a comprehensive Issue/Risk Log to track risks and assign mitigation strategies. Risks are potential future events that, if they occur, would have an impact on the project, or the successful operation of the system, whereas issues are events that have occurred and must be resolved as soon as possible. The contractor shall perform an initial risk assessment jointly with the entities, identifying and assessing the probability and impact severity of all foreseeable programmatic and technical risks, and develop mitigation strategies for high and medium exposure risks.

   The Risk Management Plan shall include how risks will be identified, managed, and mitigated. The responsibilities for monitoring and review shall be clearly defined. The monitoring and review processes shall encompass, when applicable, all aspects of the risk management process for the purposes of:
   a. Ensuring that controls are effective and efficient in both design and operation.
   b. Obtaining further information to improve risk assessment.

c. Analyzing and learning lessons from risk events, including near-misses, changes, trends, successes and failures.
d. Detecting changes in the external and internal context, including changes to risk criteria and to the risks, which may require revision of risk treatments and priorities.
e. Identifying emerging risks.

The plan shall also include a template of the Risk Log that shall be used to track issues and risks and assign mitigation strategies to address each one. The contractor shall maintain the Issue/Risk Log and update it as needed. The Issue/Risk Log is an ongoing tool for the purposes of identifying, triaging, and managing risks. The Risk Log needs to be available, visible, and monitored at least weekly.

The contractor shall maintain and update the Risk Management Plan on an ongoing basis and conduct risk reviews at least bi-weekly during a program and during FFP tasks. The contractor shall assess and mitigate risks as mandated by the National Institute of Standards and Technology (NIST) 800-53 Revision 4, NIST 800-30, and subsequent updates.

The contractor shall prepare a Risk Review Report that describes risks to the system and ongoing operations including near-misses, changes, trends, and emerging risks in addition to mitigation strategies and lessons learned from risk events. The report shall also include risk reduction recommendations.

C.5.1.5 SUBTASK FIVE – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted. The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location.

Deliverables associated with this task include:

1. Trip Report

C.5.1.6 SUBTASK SIX – QUALITY CONTROL PLAN (QCP)

The Government will provide the contractor with a Quality Assurance Surveillance Plan (QASP) that will be used to monitor contractor performance. The Contractor shall develop, maintain, enforce and document a Quality Control Plan (QCP). Within the QCP, the contractor shall identify its approach for providing quality control in meeting the requirements of the TOR. Specifically, the offeror's shall describe:

1. Quality control methodology for accomplishing TO performance expectations and objectives;
2. Processes and procedures that provides high quality performance for each Task Area;
3. Approach to planning, organizing, and managing internal resources, including subcontractors to include lines of authority;
4. Methodology to identify and resolve issues and problems, including escalation procedures;
5. Rationale for tracking and reporting progress and costs and integrating the requirements of the TO; and
6. Approach to ensure cost, performance and schedule objectives adhere to task planning.

The contractor shall provide the Government with a draft QCP on which the Government will make comments. The contractor shall update the draft QCP submitted and provide a final QCP (10) workdays after receipt of Government comments.

Deliverables associated with this task include:

1. Draft QCP
2. Final QCP

C.5.1.7 SUBTASK SEVEN – TRANSITION SERVICES

C.5.1.7.1 – TRANSITION – IN

The Contractor shall develop, maintain, and implement a transition-in plan. This plan shall describe all activities necessary to ensure continuity of operations and the maintenance of service levels from task order award until operational responsibility is completely assumed in accordance with the Government approved transition plan. Phase-in transition activities shall be performed in accordance with the contractors' Government approved final transition-in plan.

The contractor shall include in their transition plan a solution that adheres to all Government and Industry Standards. Specifically:

The consolidation and integration of the engineering, design, security, and Operations and Maintenance (O&M) of the technology infrastructure, hardware, applications, software, and network perimeter (includes but is not limited to multiple sets of firewalls, switches, routers, caching servers, antispyware/antimalware/antivirus, SMTP email antivirus/SPAM filtering, web filtering)

An integrated incident management and problem resolution solution to improve the quality of service and decrease the time to resolve for Enterprise Data and Technology Solutions' consolidated customer base.

Desktop support vendor will be critical to this effort. The incident management/problem resolution process should be defined so that it is seamless to the customer.

Additionally, the transition plan shall include:

1. Planned transition activities;
2. Transition activity timelines and milestones;
3. Transition resource requirements;
4. Transition security implications;
5. Transition risks and mitigation or avoidance strategies; and
6. Transition notifications and training of users.

The contractor shall provide the Government with a draft Transition-In Plan within (10) workdays of award, which the Government will make comments. The contractor shall update the draft plan submitted and provide a final transition-in plan (5) workdays after receipt of Government comments. The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall implement its Transition-In Plan no later than (NLT) 30 work days after award.

Deliverables associated with this task include:

1. Draft Transition-In Plan
2. Final Transition-In Plan

C.5.1.7.2 – TRANSITION – OUT

The Contractor shall develop, maintain, and implement a transition-out plan. This plan shall facilitate accomplishing a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan No Later Than (NLT) 90 workdays prior to expiration of the Base Period of Performance (POP) (Section F – Deliverables or Performance, Deliverable Table). The contractor shall update the Transition Plan 30 days prior to the end of each exercised option period (Section F – Deliverables or Performance, Deliverable Table).

The contractor shall identify how it shall coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

1. Program management processes
2. Points of contact
3. Location of technical and program management documentation
4. Status of ongoing technical initiatives
5. Appropriate contractor–to-contractor coordination to ensure a seamless transition
6. Transition of Key Personnel knowledge
7. Schedules and milestones
8. Actions required of the Government

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

Deliverables associated with this task include:

1. Transition-out Plan

C.5.2 TASK 2 – PRE-MIGRATION SUPPORT

C.5.2.1 DEVELOP AND PREPARE A SYSTEMS MIGRATION PLAN

The Contractor shall develop and prepare a systems migration plan. The systems migration plan shall describe in detail the current system, licensing impacts, cloud migration sequencing, and future state system architecture and system design. The contractor shall obtain Ginnie Mae's approval for all proposed Hosting and Cloud Service Providers (CSPs). The contractor shall utilize FedRamp approved CSPs.

The Contractor shall will be responsible for working with current providers to support the migration and testing of existing applications. Prior to the migration of each system, the contractor shall perform the following pre-migration planning activities: (1) System review/fit gap analysis, (2) Evaluate software licensing and impacts, and (3) Architecture and system design

Deliverable associated with this task includes:

1. Systems Migration Plan

C.5.2.1.1 SUBTASK ONE - SYSTEM REVIEW/FIT GAP ANALYSIS

The Contractor shall review custom code to determine if native Operating System (OS) libraries are used, if not, the Contractor shall identify the need to recompile/re-design application code to modify the OS. The contractor shall review and determine if a Commercial Off the Shelf (COTS) product is available to replace locally developed applications or functions of applications. If, during the fit/gap analysis, it is determined that a COTS software product cannot be configured to meet certain entity-specific mandatory requirements, the contractor shall provide a plan to scope, design, develop, test, and implement extensions to the COTS product to accommodate the entity-specific mandatory functionality. These extensions shall reside outside of the COTS product and shall not interfere with or increase the difficulty of implementing future releases, upgrades, and/or patches to the COTS product.
The contractor shall review each identified entity's system requirements and perform a fit/gap analysis against its proposed solution. The fit/gap analysis shall include proof of concept sessions to review the out-of-the-box solution against requirements and business processes and identify the fits and gaps. The contractor shall review the results of the fit/gap analysis to assess the level of effort required to meet the gaps and shall support and generate all activities necessary to conduct the fit/gap analysis for the system, including:

a. Review of functional and other requirements.
b. Identification of potential business process impact areas.
c. Conducting proof of concept sessions and demonstrating the new system capabilities and workflow.
d. Creating fit/gap analysis and comparison reports.

e. Developing the level of effort to configure and enhance (if required through an extension) the system.

After completion of a fit/gap analysis the contractor shall produce a Fit/Gap Analysis Report. The report shall include an executive summary with detailed findings and recommendations. The report shall also include and address the following elements:

a. Requirements review results (identifying the fits and gaps).

b. Primary users and/or functional groups impacted by the gap.

c. Functional and technical gaps and a proposal for how the contractor can fill the gap

d. External connection requirements, including method and security for the system.

e. Review infrastructure configurations to determine if alternative configurations are required.

f. Identify application interconnectivity and interrelation. The Contractor shall incorporate into the design and implement a best practices approach for Business Continuity and Disaster recovery utilizing modernized architectures.

Deliverable associated with this task includes:

1. Fit/Gap Analysis Report

C.5.2.1.2 SUBTASK TWO - EVALUATE SOFTWARE LICENSING AND IMPACTS (LICENSING MANAGEMENT)

The contractor shall determine support status of existing licenses (i.e. supported or end-of-life), consolidation of licensing across all environments, and evaluate legality of using existing licenses in cloud environments. The contractor shall review and recommend licensing consolidation availability as bundled with hosted and/or cloud services.

C.5.2.1.3 SUBTASK THREE – VIRTUALIZATION

The Contractor shall virtualize all appropriate infrastructure based on Government guidance to include but not limited to network, servers and storage. The Contractor shall perform a full virtualization analysis of all data center environments prior to migration. Based on the pre-virtualization analysis, the Contractor shall determine which servers have already been virtualized and which have not. From there, the decisions whether to virtualize first in the current environment or virtualize directly in the new environment will be decided on a case-by-case by the Government, basis depending on the current infrastructure support and the complexity of the system. The Contractor shall test the successful virtualization by following the Government provided test scripts and plans to migration.

C.5.2.1.4 SUBTASK FOUR – PERFORM GO-LIVE TESTING AND CUTOVER

The Contractor shall conduct end-to-end go-live testing (i.e. test the entire system/ perform each of the applications functions) and shall mitigate any identified vulnerabilities. Prior to the system cutover (i.e. the transition from the existing production system to the new environment/cloud), The Contractor shall develop a detailed Cutover Plan to mitigate any risks involved with system transition to the new Infrastructure as a Service/ Cloud (IaaS) environment. The Contractor shall

cutover system traffic/requests to the cloud environment upon approval by the Government and coordinate with current providers to support the migration and testing of existing applications.

Deliverables associated with this task include:

1. Cutover Plan

C.5.3 TASK 3 - MIGRATION

C.5.3.1 SUBTASK ONE – CLOUD/HOSTED MIGRATION

The contractor shall coordinate with the current service providers to migrate application and services to the cloud or hosted environment. The Contractor shall serve as a cloud broker or hosting provider for Ginnie Mae. The Contractor will be required to migrate all of the key systems (major applications) identified in the Current Information Technology (IT) Environment (See Attachment A).

The following key systems (major applications) Modernized Ginnie Mae Portal and Security Infrastructure, GFAS, GNMA-WS (SharePoint), RFS, and CipherCloud have already been modernized by Ginnie Mae and are ready to be migrated once the pre-migration process is completed. Ginnie Mae is currently working on the completion of the modernization of the remaining key systems (major applications) GMEP, GNET, and IPMS. Ginnie Mae anticipates completion by December 31, 2018.

Although specific migration activities required to move a system to the cloud will vary depending on the unique specifications, software, and configuration of each system the Contractor shall provide a cloud migration status report including a sequencing plan for the migration and shall seek Ginnie Mae approval before executing the plan.

Deliverables associated with this task include:

1. Cloud Migration Status Report

C.5.3.2 SUBTASK TWO – ESTABLISH INFRASTRUCTURE AND OPERATING SYSTEMS (OS)

Once application environments have been virtualized and the cloud architecture is defined, the Contractor shall provide the required Virtual Machines (VMs) based on the detailed system requirements during the Pre-Migration phase. The contractor shall develop and maintain a secure and certified Gold Image for all Operating Systems utilized. The contractor shall configure the Operating Systems (OS) of provisioned VMs to comply with government standards and regulations.

C.5.3.3 SUBTASK THREE – MIGRATE AND CONFIGURE DATABASE AND SOFTWARE

The Contractor shall provide the installation and provisioning of the database platform for any system identified for migration. Additionally, if the migration requires a move (change) between database products (technology), the Contractor shall assist the Government and current contractors with transforming the Data (Layout) and/or Schema. Following the database preparation, the Contractor shall migrate and validate the migrated data. To assist with the migration of the system software, the Contractor shall be prepared to install, validate, and configure software installation,

providing support for custom code modification where necessary. The need for assistance will be determined during the data layout and/ or schema transformation process.

C.5.3.4 SUBTASK FOUR – Database and Software Performance Remediation

The Contractor shall work closely with Ginnie Mae to determine if all or portions of the system (i.e. database) can reside in the cloud environment or need to be moved to an alternative virtualized or physical hardware environment managed by the Contractor that meets or exceeds application government security requirements.

C.5.3.5 SUBTASK FIVE – INTEGRATE SYSTEMS

The Contractor shall configure the necessary interfaces to external systems once the database, application, and its data have been migrated to the cloud environment. Necessary interfaces requiring configuration will be determined during the design of the platform. Once changes have been made to the integrated components and systems, the contractor shall validate the connections by conducting testing.

C.5.3.6 SUBTASK SIX – INSTALL AND CONFIGURE TOOLS AND UTILITIES

The contractor shall develop, install, configure, and if applicable update monitoring tools for the new environment in accordance with Government IT Security Standards. The Contractor shall conduct performance testing and diagnosis monitoring to validate proper installation and functionality of the tools. Approval by Ginnie Mae is required only when the tools offered by the CSP are not sufficient for Ginnie Mae's needs.

C.5.3.7 SUBTASK SEVEN – ESTABLISH USER ACCESS AND SECURITY CONTROLS

Once the Cloud Environments have been properly configured, the Contractor shall grant the appropriate access levels for cloud-hosted data and applications. In addition, the Contractor shall perform security scans and mitigate identified vulnerabilities (in accordance with NIST and agency standards). Finally, the Contractor shall compile the Certification and Accreditation Package to validate the security of the system in accordance with HUD and Ginnie Mae Policy.

C.5.4 TASK 4 – DATA CENTER SUPPORT

The contractor shall provide Ginnie Mae with technical management and systems engineering support so Ginnie Mae can more efficiently and effectively develop, integrate, acquire, manage, and operate the business and information technology systems that are critical to the services it provides to include:

1. Software Test Site Development, Management, and Operations
2. Infrastructure Engineering and Operations
3. Information Assurance and Security
4. On-going recommendations for improvements to technology, infrastructure, and processes to ensure Ginnie Mae remains current with the latest technologies

The contractor shall provide a monthly System operation and maintenance (O&M) status report relating to all activities being performed related to operations and maintenance, after systems are fully migrated to the cloud. The contractor shall ensure all operations meet the established SLA's

Deliverables associated with this task include:
1. System operation and maintenance (O&M) status reports

C.5.4.1 SUBTASK ONE – System and Network Administration

The Contractor shall work with the Cloud Service Provider to monitor the performance of the operating systems, network routers/switches, and telecommunications links to anticipate bottlenecks and to identify and resolve these whenever they occur. The contractor shall coordinate with the incumbent and perform the following activities (all activities must meet established SLA's and recovery times):

1. Ensure the routine backup of all servers can be restored to operational status from backup as necessary.
2. Manage user accounts in coordination with Help Desk and Security.
3. Apply suitable patches and upgrade system software and firmware ensuring they are kept current.
4. Ensure that all systems are up to date with current version(s) of custom application software.
5. Recommend system changes/upgrades and implementing Ginnie Mae approved changes.
6. Track and execute against approved Service Level Agreements (SLA).
7. Ensure that systems identified as Mission Critical will have an uptime of 99.99%.
8. Monitor, manage and oversee all infrastructure devices (24x7x365).
9. Provide routine and continuous monitoring of networks supporting the Ginnie environment and the administration of systems hosting software toolsets used to monitor the health of the enterprise network and systems (e.g. Windows Active Directory).
10. Provide maintenance and configuration management for all IT infrastructure including mainframes and related devices including software leases.
11. Respond, coordinate and manage all change requests for additions, removals and modifications to the environment to include maintenance coverage.
12. Maintain, troubleshoot, fix and/or replace all infrastructure devices (24x7x365).

C.5.4.2 SUBTASK TWO – Ginnie Mae Environment Support

The Contractor shall provide development, enhancement, and operation support for the Ginnie Mae environments to include DEMO, DEV, DR, PRD, QA, STG, SIT, TST, TRN, and UAT. It should be noted that Ginnie Mae is in the process of redesigning their infrastructure, so the environment could potentially change in the future. The Contractor shall leverage virtualization technology whenever possible to facilitate the management of the various environments and the need to accurately and consistently mirror the configuration of these various environments.

C.5.4.3 SUBTASK THREE – Secure the Department's critical IT infrastructures

The Contractor shall comply with all IT security and privacy for all in-scope systems, to include but not limited to: Security Assessment and Authorization (SA&A), privacy, risk analysis and mitigation, IT security and privacy baseline compliance, continuous monitoring, key escrow, audit, FOIA and e-Discovery requests, HSPD-12, forensic, breach/incident response, etc. Assist and characterize the threat environment and support development and implementation of effective countermeasures to protect and defend Ginnie Mae information networks and information.

Maintaining the availability, confidentiality, and integrity of Ginnie Mae networks and information to support Ginnie Mae operations.

The Contractor shall implement and document a program to identify, classify, and protect information associated with critical cyber assets.The Contractor shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing critical cyber asset hardware or software, and implement supporting configuration management activities to identify, control, and document all entity or vendor-related changes to hardware and software components of critical cyber assets pursuant to the change control process.

The Contractor Shall Develop and Implement Automated Cyber Security Capabilities. This will include develop, build, implement, and operate automated systems that meet the following capabilities:

a. Network Intrusion Detection, Prevention, and Analysis
b. Virus, Malware Detection and Prevention
c. Host-based End Point Protection
d. System and File Integrity Monitoring and Reportin
e. System and Network Vulnerability Scanning and Reporting
f. Centralized Patch Management and Reporting System
g. Centralized Host-based Intrusion, Detection and Prevention System
h. Centralized System and Network Log Aggregation, Correlation and Analysis

The Contractor Shall Develop and Implement Computer Network Defense (CND) / Monitor, Analyze, and Detection Services. This will include:

a. Monitor, analyze, and detect services, provide CND situational awareness, attack sensing and warning (AS&W).
b. Multiple communities within the Ginnie Mae enterprise (e.g. system administration, network operations, security, CND services) contribute to situational awareness.
c. AS&W data shall provide Ginnie Mae the ability to sense changes in the ISs enterprise.
d. AS&W includes the detection, correlation, identification, and characterization of a large spectrum of intentional unauthorized activity, including an intrusion or attack.
e. AS&W is enabled through a managed network of intrusion, misuse, and anomaly detection systems, supporting data fusion and analysis, diagnostics, long-term trend and pattern analysis, and warning communications channels and procedures.
f. Assist Ginnie Mae in developing and implementing CND policies, procedures, and guidelines that will govern day-to-day operations. This effort shall adhere to all applicable federal government directives, mandates, guidance, and publications.

The Contractor Shall Develop and Implement CND Response Service. This will include:

a. CND response services shall include the actions taken to report, analyze, coordinate, and respond to any event or cyber incident for the purpose of mitigating any adverse operational or technical impact.
b. Cyber incident reporting shall include a well-defined framework for the timely reporting of any cyber event or incident. The report provides an accurate, meaningful, and complete

understanding of the cyber incident from initial detection to analysis and remediation. This information feeds into the User-Defined Operational Picture, which provides local, intermediate, and HUD wide situational awareness of CND actions and their impact.

c. Cyber incident analysis shall identify several critical elements of an incident to determine and characterize its possible effects on Ginnie Mae information networks, operational missions, and other defense programs. This activity relies on effective acquisition, preservation, and timely reporting of cyber incident data.

d. Cyber incident response includes the coordinated development and implementation of courses of action (COAs) that focus on containment, eradication, and recovery. At the same time, it ensures the acquisition and preservation of data required for tactical analysis, strategic analysis, and/or Law Enforcement investigations.

The Contractor shall provide on-going recommendations for mitigation of all threats and risks related to the in-scope systems. The Contractor shall assist in the mitigation of any risk, directly related to any new Government policies and/or initiatives that impacts the IT infrastructure. The Contractor shall participate in the change management process and attend change management meetings. The Contractor shall also participate in Plan of Action and Milestones (POA&M) remediation, vulnerability assessment and remediation, and incident response.

The Contractor shall interface with the Ginnie Mae IT Security and Privacy Team to assure proper understanding of security and privacy policies, processes and operations. The Contractor shall participate in Plan of Action and Milestone (POA&M) remediation meetings with the Ginnie Mae System Owners, IT Development Team, and IT Developers to discuss remediation strategies, and other IT Security and Privacy related issues. POA&M is a management tool for tracking and mitigation of cyber security program and system level findings/weaknesses.

The Contractor shall comply with and provide a monthly IT Security Report to include:

a. Incident reporting comprised of well-defined framework for the timely reporting of reportable cyber event or incident. Reports shall provide an accurate, meaningful, and complete understanding of the incident from initial detection through analysis to resolution and closure.

b. Reporting shall provide valuable input into the combined and coordinated analysis of data from a variety of sources.

c. Analysis shall provide Ginnie Mae and/or other relevant stakeholders with indications of adversary reconnaissance, probing, intrusions, system and network exploitations, and /or attacks that have occurred or are occurring on Ginnie Mae IT enterprise.

d. Vulnerability scan reporting shall provide an accurate, meaningful, and complete understanding of the security posture of the Ginnie Mae IT enterprise. These reports are to be provided to Ginnie Mae at the very least 1 time per month and/or as requested.

e. Verification and Auditing: At Ginnie Mae's discretion all systems are to be available for verification and/or auditing without any interference. Relevant Ginnie Mae IT Staff shall have the ability to access, login, and perform verification and auditing of these systems and its information at any time.

The primary objectives for the incident reporting process are to:

a. Ensure all suspicious activity on Ginnie Mae IT enterprise is reported according to defined policies, procedures, and within established timeframes.
b. Ensure incident reports provide an accurate, meaningful, and complete understanding of the incident throughout its life cycle.
c. Ensure the effective and timely coordination and communication of incident information through appropriate channels.
d. Provide Ginnie Mae with the ability to direct protective and defensive strategies based on incident reporting trends and adversarial activity.

The contractor shall provide monthly a Security Report relating to all activities being performed related to securing the IT Infrastructure, after systems are fully migrated.

Deliverables associated with this task include:
1. IT Security Report

C.5.4.4 SUBTASK FOUR – Information security policy and processes

The contractor shall:
1. Evaluate and recommend security controls for Network Infrastructure (e.g. routers, switches, firewalls, VM, cloud), windows, linux and solaris environments to affected areas.
2. Evaluate and recommend controls over the Web environments.
3. Evaluate and recommend controls over the non-production environments.
4. Develop and maintain the information security policy framework for information security objectives and alignment to business and service needs and any changes/deviations to it.
5. Integrate security into the full life-cycle and workflow processes of the Department's Information Technology services.
6. Monitoring the Intrusion Detection/Prevention systems, firewalls, security event manager and other tools as necessary.
7. Develop and maintain security and network architecture that implements relevant security laws, regulations and policies.
8. Maintaining the Public Key Infrastructure.
9. Monitoring physical, environmental and information technology security.
10. Prevent the compromise of and tampering with the Department's data by safeguarding internal networks and systems from unauthorized access and hostile activity.
11. Provide daily security briefs.

The contractor shall provide documentation relating to all activities being performed related to Information security policy and processes.

C.5.4.5 SUBTASK FIVE – Certification and Accreditation (C&A) Compliance and Services / System Security Assessment and Authorization (SA&A)

The Contractor shall support Department's C&A and SA&A activities, and continuously monitor the compliance through the following steps:

1. Provide information security guidance and technical assistance.
2. Coordinate with Ginnie Mae Security Team in obtaining certification and accreditation of systems, risk assessment and remediation management.
3. Provide innovations to improve C&A compliance and monitoring.
    a. Creating C&A/SA&A artifacts including System Security Plans, System Categorization, System Boundary Diagrams, Network and Dataflow Diagrams, Risk Assessments, IT/IS Contingency Plans, Configuration Management Plans, Security Testing and Evaluation, Incident Response Plans, etc.
    b. System Categorization: FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization resulting from the operation of its information systems.
    c. System Boundary Diagram: Detailed graphic layout of the system authorization boundary.
    d. Network Diagram and Dataflow: A network diagram is a visual representation of network architecture. It maps out the structure of a network with a variety of different symbols and line connections. Data flow diagram (DFD) illustrates how data is processed by a system in terms of inputs and outputs. As its name indicates its focus is on the flow of information, where data comes from, where it goes and how it gets stored.
    e. Risk Assessment (RA): Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.
    f. Configuration Management Plan (CMP): a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems.
    g. System Security Plan (SSP): Provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system.
    h. (Information) System Contingency Plan (CP): Provides established procedures for the assessment and recovery of a system following a system disruption. The ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system.
    i. Security Testing and Evaluation (ST&E): Documents the current state of the Major Application or the General Support System in accordance with FIPS 199, NIST SP 800-

53 rev. 4, SP 800-37 rev. 1, SP 800-160 and OMB A130, A123, and FFMIA, and all future revisions.

j. Incident Response Plan (IRP): In accordance with NIST Special Publication 800-61 rev. 2, provide instructions for responding to a number of potential scenarios, including data breaches, denial of service/distributed denial of service attacks, firewall breaches, virus or malware outbreaks or insider threats.

4. Perform security scanning of all layers and remediate issues and prepare for independent testing and validation.
5. Remediate and mitigate any open issues.
6. The contractor shall provide documentation relating to all activities being performed related to C&A/SA&A.

Deliverables associated with this task include:

1. System Security Plan
2. Configuration Management Plan
3. System Boundary Diagram
4. Network and Dataflow Diagram
5. Risk Assessment
6. IS/IT System Contingency Plan
7. Security Testing and Evaluation (ST&E)
8. Incident Response Plan

C.5.4.6 SUBTASK SIX – Security of Department's Infrastructure

The Contractor shall:

1. Provide centralized patch management and end-to-end configuration management for all infrastructures.
2. Build and maintain secure enclaves to better protect sensitive data/applications from the unclassified processing environment.
3. Provide Communications Security (COMSEC) support.
4. Implement Continuous Diagnostics and Mitigation (CDM), and Einstein programs.
5. Recommend approval or rejection of proposed business system security design.
6. Recommend alternative approaches to system developers to address security issues.
7. Ensure that security best practices are utilized in the design, implementation and testing of business systems.
8. Reports as necessary or upon request showing design testing results and recommendations.

C.5.4.7 SUBTASK SEVEN – End Point Protection

The Contractor shall provide and manage the distribution and implementation of Ginnie Mae approved end point protection on Ginnie Mae virtual and physical servers.

C.5.4.8 SUBTASK EIGHT – Statement on Standards for Attestation Engagements (SSAE) 16 Audit Support

The Contractor shall perform a SSAE16 Audit through an external auditor provided by the contractor on all Ginnie Mae environments and provide results of the audit in a report. Audit criteria will be determined by the Ginnie Mae. The contractor shall be subject to a SSAE 16 issued under Statement on Standards for Attestation Engagements (SSAE) Type II Engagement Report on policies and procedures placed in operation and tests of 18 operating effectiveness of controls with AICPA SOC 1 Report (Financial Reporting) for each year of the contract term. An independent public accounting firm shall conduct the SSAE 16 report.

1. The contractor shall provide the auditor with access to all systems, information and people required to perform a SSAE 16 Type II with an AICPA SOC I review. As part of the audit process, the contractor shall provide the SSAE 16 auditor with corrective action plans for addressing any findings noted in a **SSAE 16 Audit Remediation Report**. A **draft of the SSAE 16 report** will be submitted to Ginnie Mae by August 1st of the year ordered. Each audit including follow up work shall be completed by August 30th of the year ordered. A **final SSAE 16 Audit Report** shall be completed by August 30th of the year ordered. Ginnie Mae and HUD's Office of Inspector General (OIG) shall have access to all work papers related to the SSAE 16 audit.
2. Work in conjunction with independent auditors to install auditor software to extract metrics.
3. Supply auditors with requested documents and system extracts. Typical requests include: log samples, standard operating procedures, proof of successful backup and recovery, current asset inventory, security documentation, security configuration and settings, security profiles, etc.
4. Ensure contractor technicians, security and technical leads are available for interviews with audit personnel.
5. Follow up on requests for information made during audit interviews.
6. Assist the Government in drafting responses, including technical rationale, for or against changes proposed by auditors.
7. Provide ongoing status of audit remediation activities.

Deliverables associated with this task include:

1. SSAE 16 Audit Remediation Report
2. Draft SSAE 16 Report
3. Final SSAE 16 Report

C.5.4.9 SUBTASK NINE – Server Management

The Contractor shall provide server management operations, which shall include:

1. Evaluating all new and upgraded service components or services associated with System Change Requests (SCRs) for compliance with relevant security policies, regulations, and procedures.
2. Assessing and communicating the overall impact and potential risk to service components prior to testing completion.
3. Conducting integration and security testing for all new and upgraded equipment, Networks, Software or Services to include unit, system, integration and regression testing based on requirements defined in SCRs
4. Staging new and upgraded equipment, Software or Services to smoothly transition into the existing environment based on requirements defined SCRs
5. Performing Configuration Management and Change Management activities related to Integration and Testing of SCR related systems or services.
6. The Contractor shall support the Continuity of Operations (COOP) Plan and Disaster Recovery Plan with redundant server configuration, network implementation, and fully comprehensive replication of the production environment in accordance with the COOP and DR plans.
7. The Contractor shall perform inventory management of all hardware including server installation services, verification of necessary components availability, providing adequate server space to host Ginnie Mae's applications, and providing scalable services based on performance and usage demands of the applications.
8. The Contractor shall maintain a centrally managed VM server farm to include all necessary hardware refresh, procurement activities to include purchasing, receiving, and installation of hardware, monitor hardware end of life trajectory, and system patching to triage any identified vulnerabilities or performance inhibitors.
9. The Contractor shall perform all virtualization services for the server resources including provisioning both physical and virtual servers, monitoring and distributing resource consumption effectively, and managing overall capacity.
10. The Contractor shall create reusable server configurations with typical and standard configurations. These configurations shall be continuously updated based on the latest configurations and releases.
11. The Contractor shall monitor the performance of the managed platform and the cloud platform. The Contractor shall submit a Performance Report monthly.The Contractor shall only make changes to the infrastructure and the supported application during the scheduled maintenance window. The maintenance window is currently set on the third weekend of every month. Communications shall be sent to the Government before and after the maintenance window, according to the established service level metrics.
12. The Contractor shall support the various Ginnie Mae stakeholders to install the application on the provisioned environment. The Contractor shall assist each stakeholder in their infrastructure installations and help troubleshoot any issues during the application installation and maintenance process.
13. The Contractor shall install and manage all necessary software and supporting middleware for the application.
14. The Contractor shall support the migration of services and application from the current platform to the new managed and/or cloud platforms.
15. The Contractor shall monitor the performance of the applications on the hosting platforms, including availability, performance, capacity, etc. The Contractor shall submit

a Server Management Performance Report monthly, on the first of the month. Additional reporting may be required to address findings or issues annotated on the monthly report.

C.5.4.10 SUBTASK TEN – Server Operating System and Data Services

The Contractor shall support routine and emergency changes to the operating environments based on Ginnie Mae priorities to ensure production and non-production systems remain operational and available to Ginnie Mae users. The Contractor shall maintain the current environment (virtual/physical server operating systems levels) and provide recommendations for software version levels and server capacity for as long as the Government owned servers are in use. Core server operating systems (OS) services are related to systems administration, troubleshooting, reconfiguration, scripting, and capacity analysis for the OS platforms defined below in the production, QA, test, and development environments. The Contractor shall analyze and recommend consolidating and streamlining physical and virtual server configuration if possible.

Server Operating Systems and Data Services include:

1. The Contractor shall install and configure operating systems onto servers as required by Ginnie Mae's requirements. The Contractor shall define and configure typical OS golden images with typical and standard configurations. These golden images shall be continuously updated based on the latest configurations and releases.
2. The Contractor shall set up the OS user privilege and access level based on the requirements.
3. The Contractor shall administer and maintain operating systems of the entire platform, including patching and upgrades.
4. The Contractor shall provide 24x7 monitoring of operating systems and mitigate performance incidents based on service level metrics. The Contractor shall submit a **Server Operating System and Data Service Performance Report** monthly on the first of the month. Additional reporting may be required to address findings or issues annotated on the monthly report.
5. The Contractor shall provision, install, and configure databases. The Contractor shall maintain the databases via patches and upgrades
6. The Contractor shall provide database performance tuning and capacity management services to maximize database performance. The Contractor shall submit a **DataBase Performance Report** monthly, on the first of the month. Additional reporting may be required to address findings or issues annotated on the monthly report.
7. The Contractor shall implement and maintain database security via user roles and privileges.
8. The Contractor shall maintain sound backup and recovery policies and procedures.
9. The Contractor shall provide general database support and troubleshooting and recover the database based on service level metrics.
10. The Contractor shall provide support in enabling extract, transform, and load-process in database usage and data warehousing scripts involving data within and among the third party managed platform and the Contractor's managed and cloud platforms. The Contractor shall not be providing ETL development support.

11. The Contractor shall support SAP Business Objects (i.e. a commercial off the shelf software), including but not limited to, monitoring, configuration, verification, testing, troubleshooting, and performance optimization.
12. The Contractor shall be able to encrypt data at rest and in transit using industry trending technologies through adherence to AES-256 standards.

Deliverables associated with this task include:
1. Server Operating System and Data Service Performance Report
2. Database Performance Report

C.5.4.11 SUBTASK ELEVEN – Physical Backup and Restoration Services
The Contractor shall arrange for physical backup and restoration services for all environments and sites. These include the following areas (must align with all established SLA's):
1. Maintaining, scheduling, and monitoring of incremental, full and archival backup jobs at Ginnie Mae headquarters and hosting providers.
2. Managing backup infrastructure and servers.
3. Performing archival and restoration of data as needed.
4. Maintaining transport and inventory logs of backup media.
5. Troubleshooting issues in regards to backup and recovery functions.
6. Creation of data retention policy that complies with Ginnie Mae requirements.

C.5.4.12 SUBTASK TWELVE – Virtual Backup and Restoration Services
The Contractor shall arrange for virtual backup and restoration services by the CSP. These include the following areas (must align with all established SLA's):
1. Maintaining, scheduling, and monitoring of incremental, full and archival virtual server backup jobs at Ginnie Mae hosting centers and all disaster recovery locations.
2. Managing virtual backup infrastructure and servers.
3. Performing automated site recovery restoration of data as needed.
4. Maintaining transport and inventory logs of virtual backups.
5. Troubleshooting issues in regards to backup and recovery functions for all virtual or cloud based machines.
6. Conducting semi-annual and annual routine testing of automated virtual server site recovery backups to and from Ginnie Mae hosting centers and all disaster recovery locations.
7. Creation of data retention policy that complies with Ginnie Mae requirements.

C.5.4.13 SUBTASK THIRTEEN – Virtual and Physical Database Back-up Services
The Contractor shall support all aspects of database operations for the database instances that are currently in operation and any additional instances that are created. These activities include, but are not limited to:
1. Performing routine Database backup.
2. Database tuning structures and assisting in the optimization of stored procedures as needed.
3. Generating and executing Data Definition Language (DDL) and Data Manipulation Language (DML).

4. Working with the Ginnie Mae security team to ensure user access to data is consistent with necessary role based controls.
5. The Contractor shall plan, execute, and monitor the backup of system files, data, and configurations at the frequency specified by the service level metrics.
6. The Contractor shall archive eligible data in virtual or physical tapes based on data retention service level metrics. The archived data shall be duplicated for redundancy purposes.

The Contractor shall test the back-up data, files, and server images annually. The Contractor shall ensure that system and data backups can be used for restoration purposes and that backups are not corrupt, incomplete, or unusable. The Contractor shall submit an annual Backup Data Integrity Report. The Contractor shall provide a Virtual Environment Test Failover Report NLT six (6) months after contract award. The Contractor shall provide this report semi-annually thereafter.

Deliverables associated with this task include:

1. Backup Data Integrity Report: The Backup Data Integrity Report shall include both successes and failures and include technical recommendations for improvement.

2. Virtual Environment Test Failover Report: The Virtual Environment Test Failover Report shall include both successes and failures and include technical recommendations for improvement.

C.5.4.14 SUBTASK FOURTEEN – Maintenance Management

The Contractor shall arrange for a hosting or CSP to maintain Ginnie Mae's technical infrastructure through patch management, security vulnerability remediation, and performance of system upgrades on all hardware, Operating Systems, Client Applications, and Application Services.

The Providers shall conduct, at minimum, the following activities:

1. Document all Maintenance procedures in SOPs
1. Execute plans from Engineering Support
2. Support and maintain existing practices, policies, and procedures
3. Execute remediation tasks
4. Communicate remediation status
5. Agree on best course of action until fix is available and agree on plan to implement fix when available and proved by Ginnie Mae
6. Distribute, track, and control all software changes through the release and distribution management processes and procedures
7. Document and maintain infrastructure layout

C.5.4.15 SUBTASK FIFTEEN – Configuration and Change Management

The contractor shall support the established configuration and change management practices. The contractor shall be responsible for:

1. Design, implementation and maintenance of an automated change management tool.

2. Analysis of change request impacts, including defining the associated scope, cost and schedule.
3. Providing assurances that IT infrastructure and business system changes and project documents are developed, tracked and maintained under the complete control of the agency CM tool from the beginning to the e3nd of the SDLC process.
4. The contractor shall follow the Change Control Board process, will be provided at time of award.
5. Providing estimates in hours for proposed Change Requests before work commences.
6. Providing actual hours burned upon completion of Change requests.
7. Support the Change Management Documentation process.
8. Provide reporting as required

C.5.4.16 SUBTASK SIXTEEN – Patch Management

The Contractor shall apply platform and software based patches and upgrades to all system components and make updates to security configurations based on the latest Ginnie Mae approved benchmarks or baseline standards to address new vulnerabilities and attack vectors. Under the release and deployment management services the Contractor shall:

1. Develop software release and distribution schedules.
2. Develop and distribute build program packages.
3. Ensure COTS server based applications are maintained within 2 releases of current product offerings. The Contractor shall monitor and report to Ginnie Mae the product releases and Ginnie Mae will provide direction to the Contractor regarding deployment of those releases.
4. Ensure distribution of security and application patches to the operational environment in accordance with service level agreements, NIST and HUD security policy.

The Contractor shall arrange for a CSP to provide patch management support services for all server operating system environments. The services shall ensure that newly released patches or upgrades to servers are distributed and installed as part of the release and deployment management processes and procedures. At a minimum the Contractor shall provide the following patch management services:

1. Document research & configuration baselines for all patches and version upgrades.
2. Associated integration testing processes, procedures, and documented results.
3. Patch deployment/rollout schedules and results across the various environments to minimize disruption of service in the production environment.
4. Submission of the patch to the appropriate review boards, including security, for approval.

C.5.4.17 SUBTASK SEVENTEEN – Centralized Management of the Hosted and Virtualized Environment

The Contractor shall centrally manage and secured the environments. The Contractor shall ensure physical and virtual server managed backups are centrally managed (virtual and physical can be separate, but they must be centralized). In addition, the Contractor shall create the Virtual Environment Management Report (VEMR), which verifies that the virtual environment is centrally managed. The VEMR shall be submitted within 90 days of environment creation and

submitted to the COR. The Contractor shall provide an active dashboard for government monitoring of all environments.

C.5.4.18 SUBTASK EIGHTEEN – License Management

The Contractor shall centrally manage all Commercial Off the Shelf (COTS) software licenses for all software utilized. Software in scope for this activity includes all server resident software including Operating Systems, whether run in a virtualized environment or on bare metal, virtualization software, and software components that together provide solution architecture such as databases, applications, LDAP component. Licensing compliance shall also ensure that CALs (Client Access Licenses) that are sometimes required for end users to legally access server resident software

1. Ensuring the use of all software products comply with the terms and conditions of use established by the publisher of the respective products.

C.5.4.19 SUBTASK NINETEEN – IT Service and Program management Tools

The Contractor shall suggest viable Information Technology Service Management (ITSM) and Program management tool options and offer implementation services for the selected Program management and ITSM tools. The contractor shall provide Software as a Service (SaaS) and IT Service Management (ITSM) tools. The Contractor shall act as the integrator for the Program management and ITSM tool, and provide Ginnie Mae with technical management and configuration support. The Contractor shall configure the selected Program management and ITSM tool to align with Ginnie Mae's defined processes and established tools.

Additionally, the contractor shall:

1. Design, implementation, and maintenance of an automated ITSM tool.
1. Analyze change request impacts, including defining the associated scope, cost and schedule.
2. Provide assurances that infrastructure and business system changes and project documents are developed, tracked and maintained under the complete control of the agency CM tool from the beginning to the end of the SDLC process.
3. The contractor shall follow the Change Control Board process and all related procedures.
4. Providing estimates in hours for proposed Change Requests before work commences.
5. Providing actual hours burned upon completion of Change requests.
6. Support the Change Management Documentation process
7. Provide reporting as required.
8. The Contractor shall develop, implement, and continuously improve on the change management processes and approval workflows behind the configuration changes of the managed platform and the cloud platform. The Contractor shall maintain, at a minimum, the level of service and response time as outlined in the service level metrics. The Contractor must submit a Change Request Summary NLT 5 days after completion of the configuration change.
9. The Contractor shall only make changes to the OS, supported application, and databases during the scheduled maintenance window. The maintenance window is currently set on the third weekend of every month.

10. The Contractor shall follow all program management guidance and processes as outlined in Department of Housing and Urban Development's (HUD's) Program Planning and Management (PPM) Life Cycle V2.0.
11. The Contractor shall apply Capability Maturity Model Integration (CMMI) Level 3 processes to the operations of the hosting platform. The Contractor shall provide the COR with a description of how CMMI Level 3 processes are applied to the Ginnie Mae environments in a report annually in a CMMI Level 3 process report.

Deliverable associated with this task includes:

1. Change Request Summary
2. CMMI Level 3 Process Report

C.5.4.20 SUBTASK TWENTY – IT Service and Project management Tools

The Contractor shall set up and operate a help desk to mitigate issues concerning the infrastructure of the managed and cloud platforms. The help desk shall support incident management and problem management activities. The Contractor shall utilize CMMI Level 3 processes to operate the help desk. The help desk shall be reachable 24 hours a day, 7 days a week. The help desk shall support all service level metrics.

C.5.4.21 SUBTASK TWENTY ONE – Monitoring and Reporting

The Contractor shall continuously monitor security controls of Ginnie Mae's system and its environment of operation to determine if the security controls in the information system can continue to be effective over time in light of changes that occur in the system and environment. The Contractor shall report on all Ginnie Mae systems on an ongoing basis and inform Administrators when changes occur that may impact the security of the system. The Contractor shall perform review activities and provide monthly security reports to include, but are not limited to, weekly operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of Ginnie Mae Information. The Contractor shall develop the reporting processes necessary to provide Ginnie Mae Management with real-time visibility and scoring of the security posture and its assets. The real-time visibility will be consolidated and viewable via a web interface with will allow active real-time reporting.

Multiple monitoring tools are employed by both Ginnie Mae and its current data center providers. Some are proprietary to the data center (e.g. Managed Data Center) others are Vendor-hosted (e.g. Informatica). The Contractor shall evaluate the existing monitoring tools being used and where appropriate, suggest new monitoring tools for consideration. The Contractor shall provide support for the installation and configuration of the tool(s) they elect to utilize.

C.5.4.22 SUBTASK TWENTY TWO – Network Operations

The Contractor shall provide the following network provisioning:

1. Provide Tier 2 and 3 Support for customers domestically and overseas.
    a. Tier 2: Tier 2 support shall collect information such as program name that is failed or application name or any database related details (table name, view name, package name, etc.) If a problem is new and/or personnel from this group cannot

determine a solution, they are responsible for raising this issue to the Tier III technical support group.

   a. Tier 3: Tier 3 support is responsible for handling the most difficult or advanced problems. It is synonymous with level 3 support, 3rd line support, back-end support, support line 3, high-end support, and various other headings denoting expert level troubleshooting and analysis methods. These individuals are experts in their fields and are responsible for not only assisting both Tier I and Tier II personnel, but with the research and development of solutions to new or unknown issues.

2. Provide analysis of all conditions that affect enterprise network and systems availability, reliability, performance, security and resulting recommendations and actions for continuous improvements including support for the transition of projects developed by other Ginnie Mae Contractors, into O&M. This includes development of appropriate documentation establishing operational procedures.
2. Provide and maintain a single source for users to monitor aspects of their post or site's IT infrastructure through the data provided, including Enterprise level tools currently in use.
3. Provide and maintain Department's lab and development networks. (some environments could be onsite at Ginnie Mae Facilities)
4. Provide support for the transition of projects developed by other EDTS offices into O&M, to include development of appropriate documentation establishing operational procedures.
5. Provide operations and maintenance of the contractor facilities as directed by the government.
6. Provide Continuity of Operations hardware, software and communications equipment as required.
7. Provide other Infrastructure, Platform, Storage and Software as a Service, as required.
8. The Contractor shall provide a Network Management Plan to detail the operational environment including telecommunications configuration, network administration, file transfers, and interoperability between Ginnie Mae and its business partners. This plan will describe the logical/physical environment mapping and will be updated whenever major system changes occur.
9. The Contractor shall provide all necessary wiring, cabling, routers, load balancers, switches and related network components necessary to meet Ginnie Mae's technology needs including the procurement activities to include purchasing, receiving, and installation of network hardware.
10. The Contractor shall ensure cabling meets standard requirements and is protected from failure or performance degradation.
11. The Contractor shall plan, execute, and monitor all network configuration and network administration services.
12. The Contractor shall provide comprehensive network security services to restrict network access from unauthorized users.
13. The Contractor shall provide storage area network (SAN) and local area network (LAN) services capable of supporting Ginnie Mae's technology needs.
14. The Contractor shall provide all connectivity services to include compatibility for all IPv6 services, proxy and reverse proxy services, remote access and Virtual Desktop

Infrastructure (VDI) services, point-to-point connection to external client systems, and secure dedicated connections.

15. The Contractor shall proactively monitor network connectivity and effectively utilize load balancers to maintain efficient traffic flow.
16. Ensure optimal performance of the network, to include monitoring and management of data traffic and load
17. Ongoing daily network administration task, e.g. passwords, user management, system file management, and server management.
18. Manage the design, operating system, server configurations, physical and logical files, file permissions, directory services, and user accounts.
19. Update system documentation as changes occur.
20. Provide switch, router, and VLAN, DNS, DHCP, Firewall administration, configurations, and firmware upgrades.
21. Administer all aspects of router design and edge router management – upgrade/maintenance is scheduled yearly.
22. Update the inventory of equipment to reflect changes in components.
23. Install network components as changes occur.
24. Install network hardware.
25. Conduct network infrastructure site surveys.
26. Maintain network components to include maintenance agreements.
27. Install patches.
28. Maintain the network telecommunications configuration.
29. Perform maintenance on the weekends following the first 10 business days of each month except as otherwise agreed by the Contractor and the Government.
30. In the event of an emergency, the contractor shall notify the COR and EDTS Infrastructure representatives immediately.
31. The contractor shall ensure reliable system performance on internal networks, and dedicated long distance links (e.g., T1, DS3, Eth) and other system facilities within its direct control up to the boundary with shared public networks, e.g., dial-up or other shared communications links, and shared public or Government services such as external web sites.
32. The contractor shall monitor the performance of shared communications links and servers that are outside its direct control and report any negative findings to the Government.
33. The contractor shall maintain the network equipment; keep the system current; and maintain system integrity, network functionality, and; provide high quality service to the users. At a minimum, the contractor shall perform the following system updates and installation activities:
    a. Update system software as revisions are due or new software is required
    a. Install and update network equipment
    b. Update physical layout diagrams using agency approved modeling tool(s) detailing equipment and cable routes
    c. Update system documentation, including installation configurations for each network location.
    d. Update Installation and wiring documentation for each location
    e. Update and maintain router access lists and controls

3. The contractor shall perform the following monitoring activities and report the results in a Network Monitoring Report:
    a. Monitor router uptime expressed as the percentage of operational time over the reporting period and the number of times the router was not operational.
    f. Report on all routers pertinent to RMA including those routers the contractor maintains for RMA employees and customers.
    g. Report on routers maintained by intermediary organizations outside the control of the contractor but used by the Government traffic and visible to network monitoring tools.
    h. Count and use all down time in the percentage calculations, including regularly scheduled and planned maintenance.
    i. Conduct engineering studies and performance testing and measurement of networks in order to identify performance vulnerabilities and weaknesses. The contractor shall recommend system configuration (equipment and software) updates to promote efficient and effective performance.
    j. The contractor shall document the results quarterly in a Network Performance Recommendation Report.

4. The contractor shall provide the following RMA network equipment maintenance activities. The contractor shall provide repair support during working hours, which is usually 6 AM to 5 PM central time and on call support 24 hours/day, 7 days/week.. The contractor shall respond to all calls within one hour, either in person or by phone. The contractor shall continuously monitor RMA networks as specified in the SLAs and shall respond to and remediate anomalies detected by network monitoring:
    a. Provide on-site maintenance for the LAN/WAN system, including switches, routers, cabling, etc.
    k. Monitor the network, update the system regularly, and keep the system operational and fully functional
    l. Provide maintenance (including subcontracting) through Tier 1 network manufacturers and maintenance providers
    m. Provide service needed (including subcontracting) to ensure continued network operation (e.g., specialized support from network appliance vendors)
    n. Provide router and switch maintenance for all items under OEM (Original Equipment Manufacturer) maintenance
    o. Use online network tools to maintain an inventory of the network and its user devices
    p. Provide periodic inventory reports, including assets that require maintenance as their OEM maintenance expires and deletion of items no longer in service. The contractor shall post these changes to the inventory/procurement software system
    q. The contractor shall maintain equipment maintenance records and conduct routine maintenance reviews
    r. The contractor shall provide service maintenance contracts and renew licenses and warranties as-needed
    s. The contractor shall maintain agency maintenance inventories (including subcontracting) - hard copy, soft copy, downloadable assets, CD, DVD, etc.- of licenses, warranties, software pass codes, and vendor service level agreements

t. The contractor (and any maintenance subcontractors) shall perform hardware maintenance in accordance with all warranty and manufacturer standards. Spare parts shall be kept on-site and used as needed. Where applicable, hardware maintenance shall be performed on site by the maintenance technician as part of the support services contract. Where applicable, warranty services shall be coordinated with manufacturers or resellers

5. The contractor shall utilize automated remote software distribution of COTS and Business Applications over the network directly onto designated platforms with minimal user productivity impact. The contractor shall create automated software distribution scripts.
6. The contractor shall provide the following COTS maintenance support in accordance with the terms of the COTS license agreements:
    a. Provide renovation, corrective action, vendor patch installation, and version updates to existing COTS software. The contractor shall keep the system current, maintain LAN/WAN and server platforms functionality, and ensure continued high quality service to users.
    u. Provide software security patches in a timely and efficient manner based on security requirements and FedCIRC requirements. The contractor shall respond to identified vulnerabilities and apply appropriate protection. The contractor shall monitor the global incidence of malicious software and promptly respond to any incidents with the potential to impact systems.
7. Provide ongoing service of all maintenance agreements for software and hardware and ensure timely arrangements to prevent any break in service for those tools.

Deliverable associated with this task includes:

1. Network Monitoring Report
2. Network Performance Recommendation Report

C.5.4.23 SUBTASK TWENTY THREE – Critical IT Infrastructure

The Contractor shall support Federal Government, OMB and Agency IPV6 requirements. This may include the following tasks and be included in the Migration Plan:

a. Analyze current platform for IPV6 compatibility
b. Transition planning for current platforms
c. Test and integration
d. IPV6 Conversion, implementation and Deployment

C.5.4.24 SUBTASK TWENTY FOUR – Production Applications and Databases

The contractor shall operate and maintain business systems including, but not limited to: batch processes, operating procedures (scripts), stored procedures, web applications, files, and data bases in support of the Agency's mission. Application lifecycle management changes, including emergency fixes, shall be managed and approved through the Agency's Change Management processes. All changes will be controlled within Performance shall be in accordance with the SLAs. The contractor and Government will baseline and document metrics after task order award. The Government-provided SLAs will be revised to reflect these results. The contractor shall ensure that these performance criteria are met.

The contractor shall perform the following in support of business systems:

1. The contractor shall maintain appropriate segregation of duties when tasking its employees, the same individual cannot control processes at multiple junctures in the development, test, and production process.
2. The contractor shall assure that the SDLC is followed when maintaining or testing application systems.
3. The contractor shall control production runs of batch applications in accordance with agency-provided operating procedures and business schedules, and any additional policies and procedures provided during over the life of the Task Order as new and updated application systems are deployed in production. The contractor shall also monitor and control the operation of non-batch applications following agency policies and procedures.
4. The contractor shall perform production control functions to include: operator initiated processes, processes that run automatically under other automated job scheduling facilities, restarts of abnormally terminated jobs initiated by either the operator or scheduler, and the addition or removal of processes to the scheduler. Processes may be initiated daily on demand or on a scheduler as part of cyclical operations (monthly, quarterly, annually, etc.). The contractor shall retain electronic logs generated by business applications for a minimum of 12 months. For processes initiated by the operator (either manually or as a restart), the contractor shall create and maintain an electronic log that contains the date and time the process was executed, the CR or individual authorizing the process, and the final dispensation. The operations log shall be retained for a minimum of 12 months.
5. Components migrated to test and production shall be tested so there is a reasonable assurance they will process as required for multiple cycles until business rules change or the underlying DBMS or operating software version is upgraded.
6. Substantive changes to business systems shall be integration tested to assure both upstream and downstream processes are not negatively impacted. Changes that impact high traffic, or high resource applications shall be appropriately stress and performance tested. Integration and stress test results will be provided to the CIO CM Manager and significant performance variances noted. The contractor and Government shall assess the performance impacts of any new or updated systems and agree to any revisions to system performance level requirements before migration to production occurs. Final revision decisions are the Government's. The Government will modify the SLAs accordingly.
7. The contractor shall assure complete coordination between its infrastructure and application systems teams so the Government is kept apprised of environmental changes or shutdowns that will impact the Government's ability to do business including meeting key business deadlines. Development, test, and production environments shall be available at all times, except as otherwise agreed by the contractor and the Government.
8. Manual database changes shall be an exception performed only under extreme conditions. No such change shall be undertaken or facilitated by the contractor without documentation as to what was modified, why, and the approving party via the Agency's CM system and processes.
9. Once reengineered systems are in steady state, as defined by OMB 300, the contractor shall perform regular updates in the form of software development and enhancement. Changes occur each crop year involving different insurance products, terms and

conditions, and other functional changes. Generally, there may be between 12-16 new risk management products, e.g., insurance policies for crops not previously covered, the contractor shall also implement these processes as released.

10. In the event key business processing timeframes cannot be met, the contractor shall provide technical alternatives, short-term solutions, or workarounds to facilitate the Agency's mission.
11. The contractor shall correct software problems with newly-developed code and the legacy systems in order to continue efficient operations of the systems. The contractor shall use Agency Change and Configuration Management tools to integrate and manage Configuration Control Board approved software changes.
12. The contractor shall maintain an up-to-date electronic copy of operating instructions for all business applications, subsystems, and systems maintained or developed over the life of the contract. Instructions should detail the inventory of applications, databases, files, and other component parts utilized in the process, as well as restart and recovery instructions.
13. All legacy systems are scheduled for shutdown, the contractor shall execute Government approved plans to enable a graceful shutdown that includes retirement and disposal of code assets and recovery, conversion, and migration of data.
14. Deliverables for this task shall consist of revised code, scripts, databases, and other objects and their byproducts (reports, screens, files) as directed in authorized change requests.

C.5.4.25 SUBTASK TWENTY FIVE – Technology Advancement

The Government is interested in remaining current and knowledgeable in the latest industry trends that affect the information technology provided to their customers. When requested, the contractor shall provide White Papers and Briefings to agency management, to include the following information:

1. The latest industry trends in the functional areas supported under this task order. The contractor shall provide suggestions for change to the operation and configuration of the infrastructure environment, as appropriate and as required, that will ensure that the agency remains current, efficient, and effective and so that the users continue to receive a high level of quality support. The white paper should include a cost benefit analysis of the suggested change.
2. Research and identification of system requirements and recommendations of technology solutions to EDTS staff.
3. Research and investigation of new technologies and their possible use with the agency systems. Services shall include ongoing evaluation of current technology, platforms, and operations to seek improvement and optimal business processes. The contractor shall identify and recommend best practices and best technology for the Government needs and responsibilities. For example, the Government has recently incorporated GIS technologies into its business application and expects to expand the use of this and other technologies such as Precision Farming.
4. Minimally, twice a year and where functional or performance problems appear), the contractor shall provide Ginnie Mae with white papers describing specific issues such as areas of possible cost savings or state of art IT approaches that would improve performance or reduce costs. The contractor shall evaluate system performance in

conjunction with communications and application performance. The contractor shall work with system administrators to analyze the performance of the agency developed applications, to include determining effects on server and network capacity as applications are deployed.

Deliverable associated with this task includes:

1. White Papers
2. Technology Refresh Report

C.5.4.26 SUBTASK TWENTY SIX – Log Management and Data Correlation

Log Management system

The contractor shall develop, implement, and maintain an automated Log Management system that is compatible with multiple platforms deployed within the environment and highly scalable with intuitive, actionable dashboards, predictive analytics and broad third-party extensibility, providing operational visibility and increase the level troubleshooting. The Log Management System shall:

1. Integrate with current virtualization platform and other vendors to provide proactive management capabilities to infrastructure and applications across physical, virtual, and cloud environments.
2. Collect, correlate, and analyze all types of machine-generated log data.
3. Provide a GUI-based interface that makes it easy to run simple interactive searches, as well as deep analytical queries for quick insights that provide immediate value and improved IT efficiency.

Service Catalog

The contractor shall develop, implement, and maintain an automated IT Service Catalog that delivers personalized infrastructure, applications and custom IT services. The IT Service Catalog shall:

1. Automate the end-to-end delivery and management of infrastructure, and accelerate application deployment and releases.
2. Provision and manage multi-vendor, multi-cloud infrastructure and applications by leveraging existing infrastructure, tools and processes.
3. To Ensure that requesters receive the right size resource or application at the appropriate service level for the jobs they need to perform.
4. Provide consistent, automated delivery and management of IT services and reduce time-consuming, manual processes.
5. Reclaim inactive resources for reuse with automated reclamation, providing cost savings.

IT Financial Management (ITFM)

The contractor shall develop, implement, and maintain an automated IT financial management (ITFM) tool that provides transparency and control over the costs and quality of IT services, enabling the CIO to align IT with the business and to accelerate IT transformation. The ITEM shall:

1. Provide the baseline data necessary to understand ROI and TCO for complex initiatives, including application rationalization, data center consolidation, storage optimization, end-user computing and hybrid cloud services.
2. Enable IT to meet the business expectations of the line-of-business relative to the portfolio of available services and their costs, shifting from a technical orientation to a business orientation

C.5.4.27 SUBTASK TWENTY SEVEN – DISASTER RECOVERY PROGRAM SUPPORT

The Contractor shall implement a Disaster Recovery (DR) Environment. The DR functional requirements are as follows:

1. The DR Environment shall be geographically diverse from any production site. The disaster recovery environment shall be at least one hundred and fifty (150) miles away from the production environment.

2. The DR Environment shall be a direct and unaltered replica of the production environment; non-production environments can deviate from standard only upon Ginnie Mae's approval.

3. The DR site environment shall support asynchronous mirroring of the production environment as specified in established SLA's.

4. The DR Environment shall be a direct and unaltered replica of the production environment; non-production environments can deviate from standard only upon Ginnie Mae's approval.

5. The DR site shall be capable of synchronizing the data back to the primary site to make sure data integrity is preserved.

6. The DR Environment shall be functional for a consecutive length of forty-five days. (i.e., the disaster recovery environment may be tested in production, full failover, fully functional for a minimal period of 45 days supporting normal business operations.

The contractor shall be responsible for the following:

1. The Contractor shall evaluate current disaster recovery site configurations and determine the need to maintain multiple or separate disaster recovery sites for each system. If sites can be consolidated the Contractor shall develop a disaster recovery environment to meet the minimum uptime.

2. The Contractor shall be responsible for establishing and configuring Disaster Recovery Environments for each Ginnie Mae environment (UAT, PRD, etc…) as required and determined by Ginnie Mae.

3. The disaster recovery process shall support newer methods and processes (i.e. imaging the original cloud environment, provisioning the alternative infrastructure, and building those environments based on the images, snapshots, VMWare DRS).

4. The Contractor shall provide accessibility to the alternative environments.

5. The Contractor shall conduct snapshots of the VMs to back them up at the alternative site, which can be restored when requested by Ginnie Mae.

6. The Contractor shall plan, execute, and report on disaster recovery environment testing and failover testing twice a year.

7. During a production environment failure, the contractor shall maintain the uptime requirement by failing over to the disaster recovery environment and recover the latest recoverable back up.

8. The Contractor shall maintain, schedule, and monitor incremental, full and archival virtual server backup jobs at Ginnie Mae hosting centers and all disaster recovery locations.

9. The Contractor shall automate the disaster recovery fail over processes. The Contractor shall perform a Live Production Site Failover Test every six months for each system. If the primary site goes down, the failover site to the DR site must maintain operations and conform to establish SLA's. The contractor shall provide a Disaster Recovery report 10 days after site failover test.

Deliverables associated with this task include:

1. Physical Snapshots of VMs
2. Disaster Recovery Plan
3. Disaster Recovery Report
4. Disaster Recovery Test Scenarios
5. Disaster Recovery Test Process

C.5.4.28 SUBTASK TWENTY EIGHT – BUSINESS CONTINUITY PROGRAM SUPPORT

The Contractor shall be responsible for establishing and supporting a Business Continuity program. In support of the Business Continuity Program the Contractor shall:

1. Provide a Continuity of Operations (COOP) Plan within 90 days after contract award to outline the process and procedures that will be undertaken to maintain the infrastructure services and operations under this contract during a wide range of emergencies, including localized acts of nature, accidents and technological or attack-related emergencies. The COOP Plan shall align with FedRAMP and NIST guidelines. The COOP Plan shall explain the methodologies that will be utilized to maintain the uptime requirement of the platform and to minimize business impact.

2. During a production environment failure, the Contractor shall maintain the uptime requirement by failing over to the disaster recovery environment and ensuring current production data is up to date or can be recovered via the latest recoverable back up.

Deliverables associated with this task include:

1. Continuity of Operations Plan (COOP)

C.5.5 TASK 5 – MAINTENANCE SERVICES

The contractor shall maintain hardware and software components, to include to: maintenance services, licenses, and warranties.

The contractor shall perform a procurement requirements analysis which addresses recommendations for hardware/software maintenance services, licenses, and warranties. The analysis shall specifically, cite the reason for the maintenance updates, potential risk associated with updates, licensing and warranty terms of the item, ensure the item is compliant with Section 508 of the Rehabilitation Act (as applicable) and proof of adherence to GNMA procurement policies and procedures. The contractor shall provide a Procurement Requirements Analysis Document to the Government with the results from the Procurement Requirement analysis.

Deliverables associated with this task include:

1. Procurement Requirements Analysis Document

C.5.6 TASK 6 – HOSTING SERVICES

The Contractor shall provide the infrastructure needs for the agency's comprehensive technology portfolio. The infrastructure is defined as the entire technology stack from the application and below the Operating System level. Ginnie Mae expects that the Contractor shall provide both managed hosting services and cloud hosting services, all on an integrated platform for Ginnie Mae. The Contractor shall provide, install, configure, and maintain all hardware and software necessary for the operations of the managed and cloud platforms. All assets shall be logged and maintained by the Contractor and provided to the Government as-a-service. Existing assets may be relocated to the new hosted facility if applicable to the support of Ginnie Mae environments.

C.5.6.1 SUBTASK ONE – Facilities and Support Services

1. The Contractor shall provide a Data Center Facility that meets the requirements for an Uptime Institute Tier III facility or higher. A Tier III or G2 certification or equivalent requirements must be met to include at a minimum:
    a. N+1 system component redundancy for all equipment
    b. 1 normal and 1 alternate distribution path serving the site's computer equipment
    c. Ability for each component and element of the distribution path to be removed from service on a planned basis without causing any other computer element to shut down.
    d. Concurrently maintainable computer hardware.
    e. UPS power services
    f. Emergency power systems
    g. Dual power inputs for all elements as defined by the Institute's Fault Tolerant Power Compliance Specifications Version 2

h. 99.98% availability
i. Dedicated site infrastructure to support IT systems.
j. Uninterruptible power supply (UPS) unites to filter power spikes, sags, and momentary outages.
k. Dedicated cooling equipment that continues to operate after normal office hours.
l. Engine generator to protect IT functions from extended power outages.
m. Redundant critical power and cooling components to provide select maintenance opportunities an increased margin of safety against IT process disruptions that would results from site infrastructure equipment failures (e.g. UPS modules, chillers or pumps, and engine generators).
n. Data center requires no shutdowns for equipment replacement and maintenance.
o. Redundant delivery path for power and cooling is added to the redundant critical components so there is no impact on IT operation for shutdown environments.

2. The Contractor shall provide a Data Center Facility that meets FedRAMP requirements. A FedRAMP certification or equivalent requirements incorporating NIST SP 800-53 security controls must be met to include at a minimum:
    a. Physical and environmental protection policy and procedures
    b. 24x7 Physical access authorizations and control
    c. 24x7 Physical access monitoring including intrusion alarms and surveillance equipment
    d. Access control for transmission medium and output devices
    e. Visitor access records
    f. Emergency shutoff, power, and lighting
    g. Fire protection services including suppression devices and systems and automatic fire suppression
    h. Temperature and humidity controls
    i. Water damage protection
    j. Delivery and removal
    k. Alternate work site
    l. Fully comprehensive Awareness and Training (AT) protocol to include security awareness and training policy and procedures, role-based security training, and security training records.
    m. Complete Audit and Accountability (AU) protocol to include audit and accountability policy and procedures, audit review, analysis, and reporting, and audit generation.
    n. System and Information Integrity (SI) protocol to include system and information integrity policy and procedures, information system monitoring, and malicious code protection.
    o. Physical and Environmental Protection (PE) to include physical and environmental protection policy and procedures, physical access monitoring and control, and visitor access records.
    p. Mitigate the risk arising from use of information and information systems in the execution of missions and business functions
    q. Monitor security controls for federal information systems and document security controls for all federal information systems

r. Implement a set of baseline security controls based on FIPS 199, tailor the baseline security controls based on needs, and supplement the security controls based on an organizational assessment of risk
s. Implement a set of safeguards to protect the confidentiality, integrity, and availability of the federal information system and its information

3. The Contractor shall submit an annual proof of the successful delivery and approval FedRAMP Self-Attestation Package to verify their continued FedRAMP accreditation standing.
4. The Contractor shall maintain the list of authorized personnel with physical and virtual access to the managed and cloud platforms. The Contractor shall also maintain a log of the physical entry/exit and virtual log-in/log-out to the managed and cloud platforms. These shall be summarized in a monthly Platform Access and Entry Log.
5. The Contractor shall provide a Data Center Facility that meets Leadership in Energy and Environmental Design (LEED) Building Design and Construction Certification requirements and Federal Green IT mandates such as the Energy Independence and Security Act of 2007 (EISA 2007), Executive Orders 13423 and 13514 and the Environmental Protection Agency (EPA) ENERGY STAR Data Center Energy Efficiency Initiatives.
6. The Contractor shall meet the IT policy and procedure guidelines set by the HUD Information Technology Security Policy (2400.25 REV4) to promote security in the development, operation, maintenance, and support of all HUD IT resources to include at a minimum:
    a. Control physical access authorizations to facilities
    b. Secure and maintain control of access to high-impact system transmission lines
    c. Maintain control of access to devices displaying information on high-impact systems
    d. Monitor physical access to HUD information systems and respond to incidents
    e. Review and maintain visitor access records for facilities where HUD information assets are housed
    f. Protect power equipment and cabling for HUD information systems
    g. Provide capability of shutting off power to HUD information systems in the event of an emergency
    h. Provide uninterruptable power supplies to be used to allow for the proper shutdown of HUD information during an emergency
    i. Provide automatic emergency lighting in facilities that house HUD information systems
    j. Provide fire detection and suppression mechanisms in facilities that house HUD information systems
    k. Monitor and maintain acceptable temperature and humidity levels in facilities that house HUD information systems
    l. Maintain mechanisms to protect HUD information systems from water damage in the event of faulty plumbing
    m. Control the delivery and removal of information system-related items, as well as maintain documentation of these activities
    n. Maintain appropriate security controls at alternate work locations

o. Consider the placement of HUD information system components within facilities to minimize potential physical damage to the components
p. Protect information assets and restore services with minimal disruption during an emergency
q. Sustain contingency planning policy and procedures that are consistent with all other HUD policies, applicable laws, Executive Orders, Directives, policies, regulations, standards, and guidance
r. Develop and maintain Contingency Plans and Business Impact Assessments for HUD information systems
s. Provide training in contingency planning procedures and logistics for all personnel involved in information system contingency planning
t. Conduct testing of contingency plans for HUD information systems on a regular basis
u. Identify alternate sites for storage of information system backups
v. Identify alternate sites for the resumption of information system operations in the event of a disaster or major disruption of services
w. Identify alternate telecommunications services for the resumption of information system operations in the event of a disaster or major disruption of services
x. Conduct backups of system-level and user-level information contained in the information system
y. Implement policies and procedures for the recovery of an information system after a disruption
z. Monitor physical access to HUD information systems and respond to incidents.
aa. Sustain contingency planning policy and procedures that are consistent with all other HUD policies, applicable laws, Executive Orders, Directives, policies, regulations, standards, and guidance.
bb. Identify alternate telecommunications services for the resumption of information system operations in the event of a disaster or major disruption of services.

7. The Contractor shall provide security services that include packaging classified information, mailing and receiving classified material, implementing emergency procedures for protection of classified information security checks and internal security controls for protection of classified material and high-value property.
8. The Contractor shall demonstrate, at the time of contract award, ownership of the hosting and DR facilities, or proof that the facilities are leased past the base year and subsequent option year(s) of the contract.
9. The contractor shall provide configuration management, hardware management, operating system and system software support, and platform operations support for all application hosts.
10. The contractor shall provide on-call (e.g., pager or cell phone) system operations support 24 hours/day, 7 days/week. The contractor shall respond, either in person or by phone, to all calls within two hours. The contractor shall record off-hour calls and responses using the problem management system no later than the next business day.
11. The Government uses Web technologies for information transfer. The contractor shall support e-commerce, encryption over the Internet, intra and inter agency transfer of funds and information, and emerging technologies. The contractor shall maintain and administer applications host environments and peripheral support functions to allow the

agency and its customers to fully use the applications. The contractor shall provide support for Internet, Intranet, and Extranet environments.

12. The contractor shall be capable of administering software within the Microsoft, Linux, and Solaris environments.
13. The contractor shall operate and maintain the application systems and data bases before and after the application systems are re-engineered in accordance with the SLAs. The contractor and Government will baseline and document response time, turnaround time, and throughput after task order award. The Government-provided SLAs will be revised to reflect these results. The contractor shall ensure that these performance criteria are met. The contractor shall perform the following in support of application software and databases:
    a. The contractor shall control production runs of batch applications in accordance with agency-provided operating procedures, including the procedures and any additional procedures provided during the life of the Task Order as new and updated application systems are deployed in production. The contractor shall also monitor and control the operation of non-batch applications following agency procedures.
    b. Production Control, including operator initiated systems, applications that run automatically such as backup, and both routine daily and cyclical periodic (monthly, quarterly, annually, etc.) job schedules. The contractor shall support ad hoc job execution as requested by users or systems staff.
    c. The contractor shall operate subsystems (data base management systems, servers infrastructure, operating system, dispatchers, and other system software) such that both interactive and batch applications are accessible for production use at all times. The contractor shall operate these subsystems to provide development, test, quality control, and acceptance of new and updated applications in accordance with schedule agreements. Development and test environments shall be available at all times, except as otherwise agreed by the contractor and the Government.
    d. The contractor shall ensure reliable system performance on servers and other system facilities within its direct control. The contractor shall monitor the performance of services that impact the network and report any negative findings to the Government.
    e. The contractor shall test new and updated application systems, including performance testing, as provided elsewhere in the Task Order. The contractor and Government shall assess the performance impacts of any new or updated systems and agree to any revisions to system performance level requirements (response time, turnaround time, and throughput). Final revision decisions are the Government's. The Government will modify the SLAs accordingly.
    f. The contractor and Government will assess performance impacts of new hardware and system software, as otherwise provided in the Task Order, and shall agree to any enhanced performance level requirements or other revisions. Final revision decisions are the Government's. The contractor and Government will assess the performance impacts of increased transaction volumes or shifts in demand patterns, and revise performance level requirements as with hardware and software updates and update the SLAs accordingly.

g. The contractor shall install software, patches, or upgrades, modify tables or databases and assist Government personnel in performing this function. The contractor shall act as a liaison between the software vendor and Government's staff to facilitate resolution of technical problems.
h. Perform nightly tape backups of the servers. The contractor shall hand deliver the backup tapes to the off-site storage provider. The contractor shall place tapes that are stored on-site in the storage cabinet located in the computer room and maintain all records regarding the whereabouts of all storage media at all times. Restores shall be simulated by testing back-up tapes monthly to assure backup files and data are recoverable. Tapes from these back up operations shall be included in the overall off-site storage of data.

Deliverables associated with this task include:

1. FedRAMP Self-Attestation Package

C.5.6.2 SUBTASK TWO – DATABASE MANAGEMENT

The contractor shall administer and manage the databases for the legacy systems and the reengineered system. The contractor shall use the agency provided database tools to provide this support. At a minimum, the contractor shall provide the following types of database support:

a. Database construction
b. Maintenance
c. Back-ups
d. Database space allocation
e. Data warehousing

C.5.6.3 SUBTASK THREE – EQUIPMENT

The contractor shall maintain the hosting equipment; keep the system current; maintain system integrity, functionality, and; provide high quality service to the users. At a minimum, the contractor shall perform the following system updates and installation activities:

a. Update system software as revisions are due or new software is required.
b. Install and update server equipment.
c. Update physical layout diagrams using agency approved modeling tool(s) detailing equipment and location.
d. Update system documentation, including installation configurations for each host location.
e. Update Installation documentation for each location.

C.5.7. TASK SEVEN – DATA CENTER ENHANCEMENTS, FUTURE SYSTEM FUNCTIONALITY

This Optional Task provides the ability for GNMA to obtain enhancements to the data center managed under this TO as well as new system functionality and additional services from the contractor**.** The Contractor will assist in the development of new technology solutions or enhancements to existing infrastructure as determined by Ginnie Mae. At Ginnie Mae's sole discretion, any of Ginnie Mae's proprietary data and automated systems, may be developed, maintained, or upgraded by a third party Contractor. The contractor shall make enhancements to

the existing Ginnie Mae infrastructure including development of new state of the art information technology solutions to support Ginnie Mae's growing business needs.

The Contractor shall provide the following services for each action approved by Ginnie Mae:

1. Manage and monitor each project activity and communicate the project status to the COR and appropriate SME in writing.
2. Prepare draft approval reports, which record the authorization by the COR for the technical change request to be completed.
3. Perform requirements and benefits analysis for each enhancement as required.
4. Perform analysis, design, development of enhancements, modifications, and implement enhancements to existing systems. Contractor will coordinate any changes through Ginnie Mae's Change Control Board.
5. Implement service modifications, enhancements, upgrades to new or existing technology, secure software licenses, subscriptions, data, etc., to meet Ginnie Mae's requirement.
6. Perform analysis, design, and development for proposed new systems, products and processes.
7. Design, develop or update user manuals, training manuals and other related documentation.
8. Design and develop test plans for each enhancement, conduct the test and report the results to the GTR and appropriate GTM.
9. Perform quality assurance activities to ensure that a high quality enhancement is produced that are free from defects.
10. Provide the hardware and software upgrades to support new business needs.
11. Upgrade or implement new technologies to support existing or new programs and products, including communication lines, peripheral equipment, etc.
12. Maintain and update system documentation.

Deliverable associated with this task includes:

1. Requirements and Benefits Analysis Report
2. Test Plan

C.7 CONSTRAINTS

The successful offeror shall perform all work in accordance with the Ginnie Mae Service Level Agreement Metrics, National Institute of Standards and Technology (NIST) SP 800-53, Federal Information Security Management Act (FISMA) and Federal Information System Controls Audit Manual (FISCAM) guidelines and regulations. The successful offeror shall have the following certifications: Federal Risk and Authorization Management (FEDRAMP), uptime and/or International Data Center Authority (IDCA), and Capability Maturity Model Integration (CMMI) Level 3. The successful offeror shall perform all work in accordance with the HUD IT Security Policy. The successful offeror shall ensure that Information Technology Infrastructure Library (ITIL) methodologies are incorporated into the Program management structure and guide the overall execution of the requirements. The successful offeror shall ensure that all systems are 508 compliant. The successful offeror shall provide a Data Center Facility that meets Leadership in Energy and Environmental Design (LEED) Building Design and Construction Certification requirements and Federal Green IT mandates.